REMARKS

In accordance with the foregoing, the specification and claims have not been amended. No claims have been cancelled. Claims 1-15 are pending and under consideration.

ALLOWABLE SUBJECT MATTER

Claims 13-15 were indicated as allowable if rewritten in independent form. Applicants acknowledge with appreciation the indication of allowable subject matter. However, since Applicants consider that claim 1, from which claims 13-15 depend, defines patentable subject matter, claims 13-15 are maintained in dependent form at the present time.

RESPONSE TO REMARKS/ARGUMENTS

Claims 1-12 are rejected under 35 U.S.C. 102(e) as anticipated by U.S. Patent No. 6,937,727 to Yup et al. (hereinafter "Yup").

On page 3, item 4 of the outstanding Office Action, the Examiner acknowledges that in the Response filed by Applicants on January 19th, 2006, Applicants argued that Yup does not teach or suggest:

- "a first selector that segments input data into execution block lengths smaller than said processing block length",
- "an intermediate register/Shift Row transformation circuit that temporarily stores the output of said first Round Key Addition circuit and executes Shift Row transformation using said processing block length", and
- "a second selector that outputs to said first Round Key Addition circuit one output from among the outputs of said first selector, intermediate register/Shift Row transformation circuit, Byte Sub transformation circuit, or Mix Column transformation circuit."

However, in the "Response to Remarks/Arguments" section, only arguments that the first selector recited in claim 1 is anticipated by Yup are presented. The Office Action does not rebut the previously presented arguments that Yup fails to teach or suggest the intermediate register/Shift Row transformation circuit and the second selector of claim 1. Not addressing all the arguments related to independent claim 1 renders the Office Action defective according to 37 C.F.R. 1.104. Therefore, Applicants request withdrawal of the FINALITY of the Office Action.

The Examiner indicates the portion between col. 4, line 40 and col. 5, line 2 of Yup as teaching the first selector as recited above. The indicated portion of Yup is fully reproduced below:

> A block diagram of a circuit used to implement the Advanced Encryption Standard Rijndaeal block cipher algorithm in a system having a plurality of channels is depicted in FIG. 1. As depicted therein, the circuit 100 includes a plurality of input registers 102, one each coupled to the plurality of system channels. Although the present invention encompasses various numbers of system channels, the preferred embodiment is directed to a system having four channels. Thus, four input registers 102 are depicted in FIG. 1. The input registers 102 are preferably simple first-in-first-out (FIFO) registers, though the skilled artisan will appreciate that other types of registers could be used. **The input registers 102 each receive a data string of a first predetermined bit length from its corresponding system channel. In the preferred embodiment, the predetermined bit length is 64 bits, though larger data strings could be used.**
>
> The circuit 100 also includes a plurality of control signal input lines 103, one for each channel, coupled to receive control signals from systems and circuits external to the circuit 100. The control signals are coupled, one each, to a plurality of finite state machine controllers (FSMs) 104. There is one FSM 104 associated with each channel, each of which, in response to the received control signals, controls the operation of the remaining portions of the circuit 100.
>
> **The input registers 102 are all coupled to a single buffer register 106. The buffer register 106, under control of one of the plurality of FSMs 104, selectively retrieves and stores a plurality of data strings of a predetermined bit length from one of the FIFO registers 102, until a data block of a predetermined bit length is stored in the buffer register 106.**

In the above-reproduced portion of Yup the references to **length** were emphasized. There is no element in the above-described structure that teaches or suggests segmenting input data. In Yup, the input data is received through the input registers 102 that are coupled in the single buffer register 106. Merging "a plurality of data strings of a predetermined bit length from one of the FIFO registers 102, until a data block of a predetermined bit length is stored in the buffer register 106" is an operation opposite to "[segmenting] data into execution block lengths smaller than said processing block length." Applicants respectfully submit that the additional portion of Yup indicated in the "Response to Remarks/Arguments" section does not teach the claimed first selector recited in claim 1.

CLAIM REJECTIONS UNDER 35 U.S.C. 102

The rejections and the arguments supporting the rejections of claims 1-12 repeat the non-final Office Action verbatim. Applicants reiterate the arguments presented in the response filed on January 19th and not addressed in the outstanding Office Action.

The present invention discloses a circuit configuration that allows for a reduced circuit size while enabling high-speed processing for implementing an AES block cipher algorithm.

Significant features of the invention include, but are not limited to, an intermediate register and a shift row transformation circuit that are commonly used. Additionally, the shift row transformation is only executed using a processing block length while other processes are executed using an execution block length. There is also included a second selector that selectively outputs a value from among a first selector, an intermediate register, a shift row transformation circuit, a Byte Sub transformation circuit, or a Mix Column transformation circuit. These features of the invention can be seen, for example, by an embodiment illustrated in Figure 4 of the present application.

Claim 1 recites "a second selector that outputs to said first Round Key Addition circuit one output from among the outputs of said first selector, intermediate register/Shift Row transformation circuit, Byte Sub transformation circuit, or Mix column transformation circuit." Yup neither teaches nor suggests this claimed limitation. As stated above, in the Office Action rejection of claim 1, the Examiner cites column 1, line 16 to column 2, line 46 in Yup to show this claimed limitation. These sections of Yup merely describe the generic AES block cipher algorithm. There is no discussion to the particular configuration of implementing the AES block cipher algorithm as recited in claim 1 and as described for the present invention.

Additionally, the remaining disclosure of Yup does not teach or suggest the claimed limitation. The present invention shows that the second selector receives input data from the first selector, the ByteSub transformation circuit, the MixColumn transformation circuit, or the intermediate register/Shift Row transformation circuit. Depending on the current processing round, the second selector is set to a different position and sends one of the above listed input values to the first Round Key Addition circuit. Yup does not remotely show the presence of a second selector. As discussed above, Yup does not suggest or disclose a first selector, let alone a second selector for sending various inputs to the first Round Key Addition circuit.

Furthermore, Yup shows a circuit in which a first AddRoundKey 116, an input register 120, a ByteSub/InvByteSub 122, a ShiftRow/InvShiftRow 124, a MixCol/InvMixCol 126, and a second AddRoundKey 118 are connected in series (see Yup, figure 1). Because of this configuration, only the value of the second AddRoundKey 118 is stored in a storage register 110. Therefore, because of the series connection and lack of individual outputs of the ByteSub circuit 122, ShiftRow circuit 124, and the MixCol circuit 126, these individual circuits cannot provide an independent input value to the second selector even if it existed in the disclosure of Yup. The invention of claim 1 indicates individual values being inputted into the second selector. As such, Yup fails to suggest or disclose "a second selector that outputs to said first Round Key

Addition circuit one output from among the outputs of said first selector, intermediate register/Shift Row transformation circuit, Byte Sub transformation circuit, or Mix column transformation circuit."

Claim 1 further recites "an intermediate register/Shift Row transformation circuit that temporarily stores the output of said first Round Key Addition circuit and executes Shift Row transformation using said processing block length." Yup neither teaches nor suggests this feature. As stated above, in the Office Action rejection of claim 1, the Examiner cites column 1, line 16 to column 2, line 46 in Yup to show this claim limitation. These sections of Yup merely describe the generic AES block cipher algorithm. There is no discussion to the particular configuration of implementing the AES block cipher algorithm as recited in claim 1 and as described for the present invention.

Additionally, the remaining disclosure of Yup does not teach or suggest the claimed limitation. Contrary to the present invention, Yup states that after the "initial transformation round, the data block is fed back to the cipher block input register 120 for the next transformation round" (Yup, column 6, lines 34-36). As such, Yup does not show an intermediate register that stores a value from the first Round Key Addition. Also, even though Yup discloses a storage register 110, this register is serially connected to the second Round Key Addition circuit. Therefore, it cannot receive the value from the first Round Key Addition circuit. The storage register of Yup also has no ability to perform Shift Row transformations, as recited in claim 1. As such, Yup fails to disclose "an intermediate register/Shift Row transformation circuit that temporarily stores the output of said first Round Key Addition circuit and executes Shift Row transformation using said processing block length."

Because Yup does not disclose each limitation of claim 1, as discussed above, it is respectfully submitted that claim 1 is patentable over the prior art. Claims 2-12 depend, directly or indirectly, from claim 1 and distinguish over the prior art at least by inheriting patentable features from claim 1.

Applicants request entry of the present Rule 116 Response and Request for Reconsideration because the finality of the Office Action was premature since arguments related to features of the claims argued as distinguishing the claims from the prior art have not been addressed.

If there are any formal matters remaining after this response, the Examiner is requested to telephone the undersigned to attend to these matters.

If there are any additional fees associated with filing of this Amendment, please charge the same to our Deposit Account No. 19-3935.

Respectfully submitted,

STAAS & HALSEY LLP

Date: June 15, 2006

By: _____
Luminita Todor
Registration No. 57,639

1201 New York Ave, N.W., 7th Floor
Washington, D.C. 20005
Telephone: (202) 434-1500
Facsimile: (202) 434-1501